PEOPLE SHOULD BE YOUR GREATEST ASSET

Regular columnist and risk expert **Annie Searle** ponders the various aspects of people risk

Annie Searle

Annie Searle is a faculty lecturer at the University of Washington's Information School, where she teaches courses she designed on operational risk, ethics, policy and law as relevant to information technology. She is also principal of Annie Searle & Associates LLC, engaged in research and consulting through the ASA Institute of Risk and Innovation.

I've written in *Risk Universe* about people risk before. In November of 2012, I asked about ethical misconduct, in particular from CEOs. I made five recommendations to improve existing programmes and reduce such conduct. Earlier this year, in June, I looked hard at law firm Lobaton Sucharow's surveys of banking professionals, from the first survey in 2012 to the current one this year. The most recent survey was even larger than the first and the results were at least as disappointing as the 2012 results: we see in each that significant numbers of US and UK bankers would engage in insider trading if they thought they would not be caught.

Here I will focus on how managers can manage people risk through a higher level of situational awareness and by being able to identify what has gone wrong and caused financial and/or reputational risk in four different scenarios.

Accidents or mistakes: this is actually the easiest people risk to manage. Should you identify a pattern, you can review your training materials, as well as your policies and procedures and then invest in additional training and clarify your procedures. If the pattern persists, or if the employees making the mistakes are not new employees, then perhaps these are not accidents or mistakes.

Deliberate: Annex 9 of the most recent Basel regulations calls this type of behaviour internal fraud: "Losses due to acts of a type intended to defraud, misappropriate property, or circumvent regulations, the law or company policy..." This covers a lot of ground. Such fraud can be reduced by investing up front during the hiring process in background checks, particularly if there are aberrations in the employment history which need to be checked. We know from the detailed research which the Carnegie Mellon University CERT Division has carried out, that managers should be especially alert when an employee's performance is downgraded and the employee feels unappreciated. If such a person has development and/or administrative privileges, the results can be very expensive for the firm. The same applies to an employee one is terminating: be sure both network and remote access are terminated. (I know, that sounds very simplistic, yet there is a whole study done by the CERT and the Secret Service who interviewed former banking employees now in jail and you would be surprised how often that might have happened: the former employee went home and still had remote access open by which damage could be done.)

Third parties: Here, the people committing the fraud or property misappropriation are contractors and vendors. I wrote about vendor risk and intellectual property in November of 2013. I am not sure the situation has improved since, unless the firm has seen a significant loss because of access that a contractor or vendor had to facilities and/or records. The Carnegie Mellon CERT has written extensively on this type of risk as

well. In point of fact, we don't do well at ensuring our contractors are walled off well enough inside our production systems (example: Target Corporation and access obtained by hackers through an HVAC vendor's credentials). Again, here we recommend good solid background checks on vendors along with detailed binding clauses in contracts signed. I would recommend each contract contain a list of subcontractors that the contractor signing the contract may be using; and the same type of background investigations conducted on the subcontractors. Then monitor your critical vendors closely.

Social media: These days every employee is a potential commentator on social media unless there is a clear policy in place which outlines what's acceptable and what is not. Are they allowed to comment on their workday? On their manager? On their company? Policies and laws may vary by sector or country. It is worthwhile to develop a clear policy that is not inconsistent with brand statements so employees do not inadvertently hurt the company when they are anxious or tired. Out of a turbulent last several years, the Seattle Police Department developed a comprehensive social media policy of many parts. Here is a small but relevant portion of the policy as it applies to officers: "The Department recognises the role that social media plays in the personal lives of some Department employees. However, the personal use of social media can have bearing on employees in their official capacity as they are held to a high standard by the community. Engaging in prohibited speech outlined in this policy may provide grounds for discipline and may be used to undermine or impeach an officer's testimony in legal proceedings."

Some corporations are currently using creepy software, where employees can report on other employees, with or without cause

A few words as I close about attempts using technology to build the "better mousetrap by which to catch them" that employee surveillance programmes use – ranging from the software which the trading desks have used for several years on traders' email; or the type of new surveillance software JPMorgan Chase announced in its annual report last year; or the creepy software which some multinational corporations currently use, where employees can report on other employees, with or without cause. Are employees aware such programmes are being used? Does that make them more or less anxious, more or less willing to cheat if they think they can get away with it? Given a range of options in the marketplace, do people want to work for companies that deploy such tools? Only time and a bit more transparency about what is actually done with the data which is collected will tell. Hire the right people and your need for such technology decreases. Inspire them to do the right thing and you probably cut the risk still further. TRU